Grover Algorithmus: Seine verschiedenen Deutungen und Implementation in einem Quantencomputer

Manuel Auer

11. November 2009

Überblick

Bedeutung des Grover Algorithmus

- Gut zum erklären der Vorteile eines Quantencomputers
- Ergebnis in O($\sqrt{N}$) im Vergleich zu klassisch O(N)

Quantengatter

Definition Quantengatter

Quantengatter sind die elementaren Operationen, die ein Quantencomputer auf seinen Qubits durchführen kann. Sie sind vergleichbar mit elektronischen Gattern, welche die elementaren Operationen eines klassischen Computers durchführen.Aus mathematischer Sicht ist ein Quantengatter eine unitäre Transformation U welche auf einen Zustand Ψ angewandt wird. Die Bedingung der Unitarität folgt aus der Erhaltung der Norm der Wellenfunktion.

Hadamard Gatter

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Hadamard Gate

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Hadamard Gatter

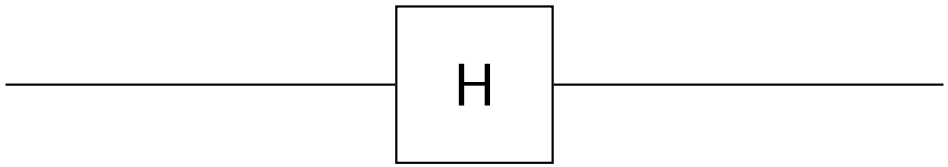


Abbildung: Circuit symbol for Hadamard Gate

CNOT Gatter

$$C|00\rangle = |00\rangle$$
$$C|01\rangle = |01\rangle$$
$$C|10\rangle = |11\rangle$$
$$C|11\rangle = |10\rangle$$

CNOT Gate

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

CNOT Gatter

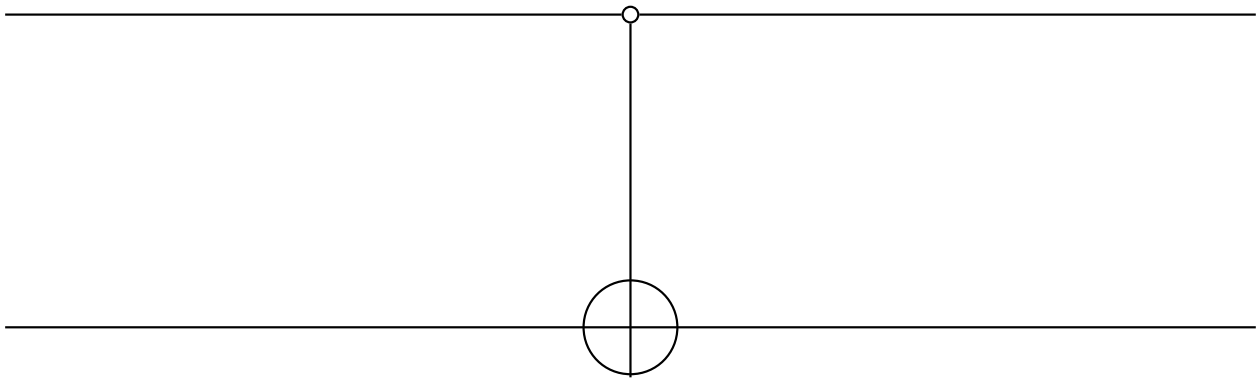


Abbildung: Circuit symbol for Controlled-Not Gate

Toffoli Gatter

Toffoli-Gate

$$T = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Toffoli Gatter

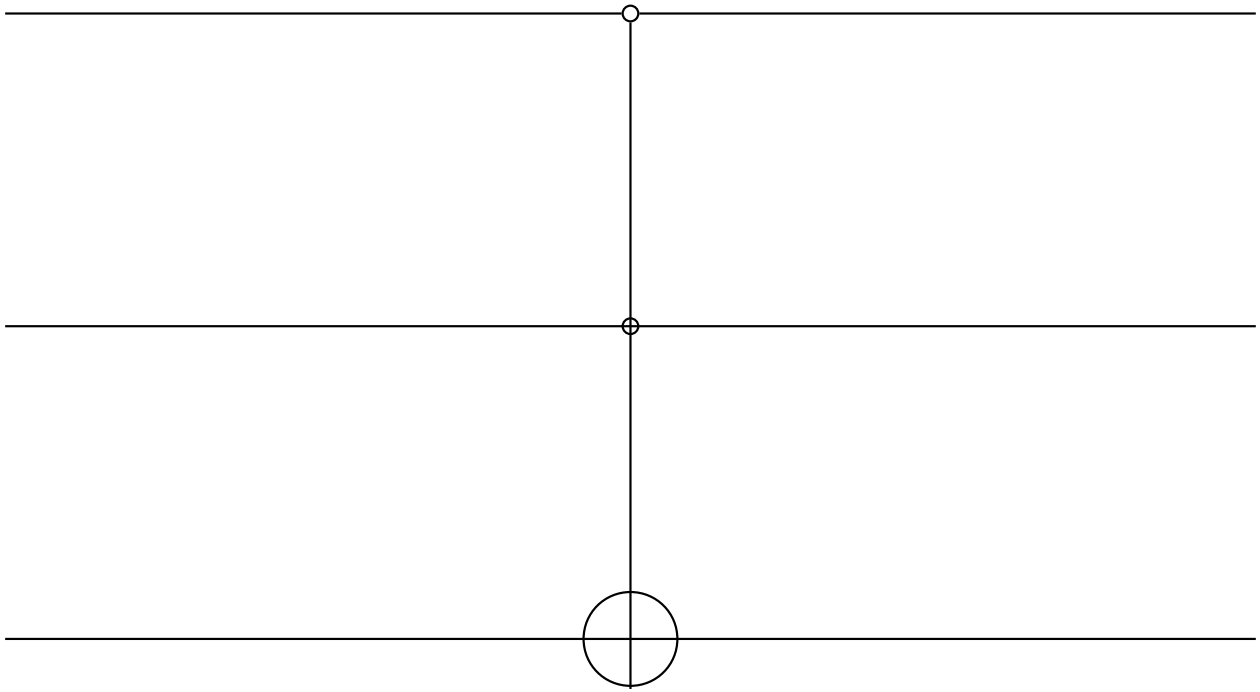


Abbildung: Circuit symbol for Toffoli

NOT Gatter

$$X|0\rangle = |1\rangle$$
$$X|1\rangle = |0\rangle$$

NOT Gate

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

NOT Gatter

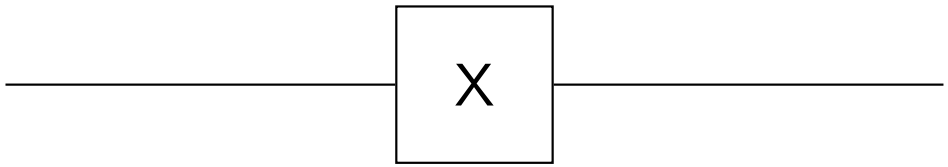


Abbildung: Circuit symbol for NOT Gate

Grover Algorithmus Überblick

Die Schritte

- Quantenregister initialisieren (Superposition)
- Anwenden des Orakels
- Anwenden des Grover Operators

Diese Schritte werden als Grover Iteration bezeichnet.

Quantenregister initialisieren

- Zwei Register (das Datenregister mit n Qubits und Das Hilfsregister für das Orakel mit einem Qubit)
- Das Datenregister wird in den Zustand $\frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle$ initialisiert
- Hilfsregister befindet sich in $|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$

Das Orakels

Aufgabe des Orakels

Das Orakel markiert das gesuchte Element indem es das Vorzeichen dieses Elementes umdreht. Dabei kann das Orakel alle verfügbaren Zustände gleichzeitig sehen, was klassisch nicht möglich wäre. Daher kann das Orakel in einem Schritt den gesuchten Zustand ausfindig machen.

- $U_f(|i\rangle|j\rangle) = |i\rangle|j \oplus f(i)\rangle$ where $\oplus$ means addition modulo 2
- $U_f = (-1)^{f(i)}|i\rangle|-\rangle$

Anwenden des Orakels

$$
\begin{aligned}
|\Psi_F\rangle|-\rangle &= U_f(|\Psi\rangle|-\rangle) \\
&= \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} U_f(|i\rangle|-\rangle) \\
&= \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} (-1)^{f(i)}|i\rangle|-\rangle
\end{aligned}
$$

wobei

$$
f(i) = \begin{cases} 0 & \text{for } i = i_0 \\ 1 & \text{for } i \neq i_0 \end{cases}
$$

Der Grover Operator

Aufgabe des Grover Operators

Der Grover Operator erhöht die Wahrscheinlichkeitsamplitude des gesuchten Elements und verringert gleichzeitig die Amplituden der restlichen Elemente.

Grover operator

$$G = 2|\Psi\rangle\langle\Psi| - I \tag{1}$$

Interprätationsmöglichkeiten des Grover Operators

- Invertierung um den Mittelwert
- Rotation des Vektors in Richtung Lösungsvektor

Invertierung um den Mittelwert

Definition

Invertierung um den Mittelwert bedeutet, dass allle Amplituden um den Mittelwert $\frac{1}{N}\sum_{i=1}^{N} a_i$ über alle Wahrscheinlichkeitsamplituden gespiegelt werden. Im Klartext heißt das, dass nach der Anwendung des Grover Operators Amplituden, deren Wert über dem Mittelwert lagen, danach um den Wert unter dem Mittelwert liegen. Das selbe gilt natürlich auch in die andere Richtung.

Vor Anwendung des Grover Operators

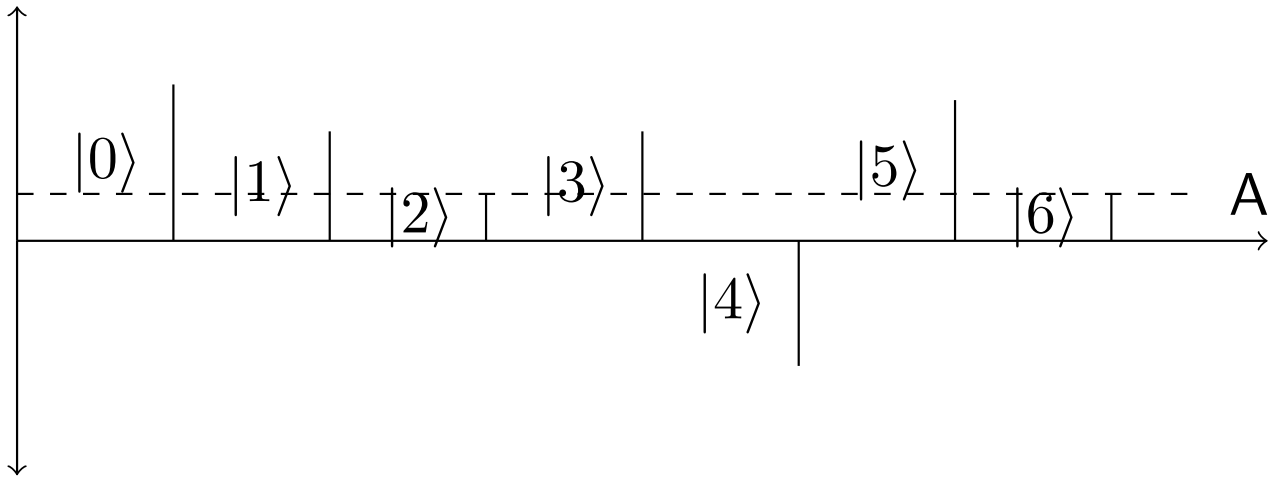


Abbildung: Before inversion about average operation is applied. Note that the only state with negative amplitude is $|4\rangle$

Nach Anwendung des Grover Operators

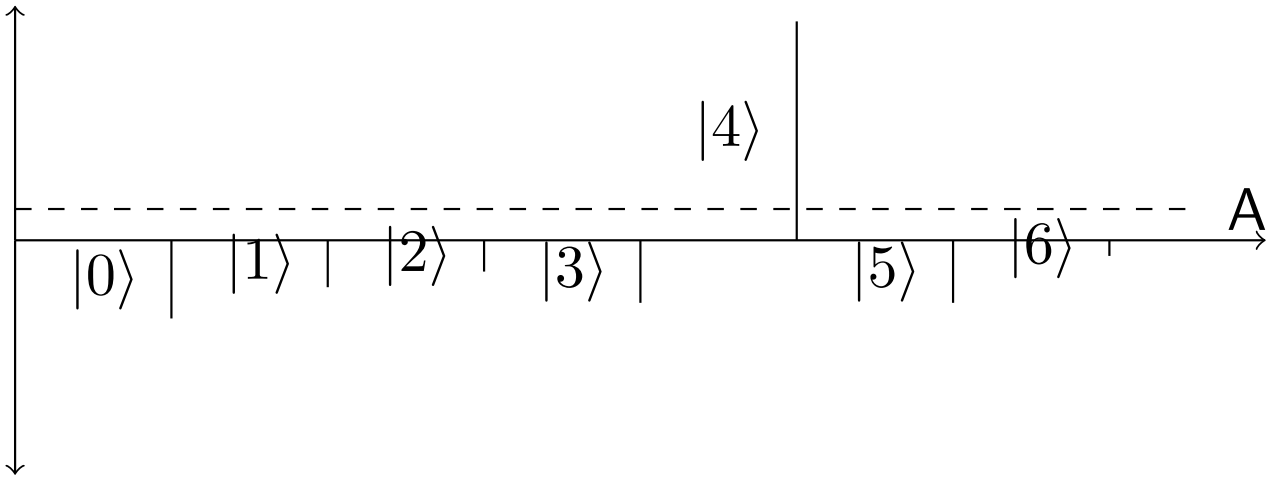


Abbildung: After inversion about average operation is applied. Note that now $|4\rangle$ is the only state whoese amplitude increased while the others have decreased in magnitude. Its also noteworthy, that the amplitudes of all states have changed sign.

Grover Operator in anderer Darstellung

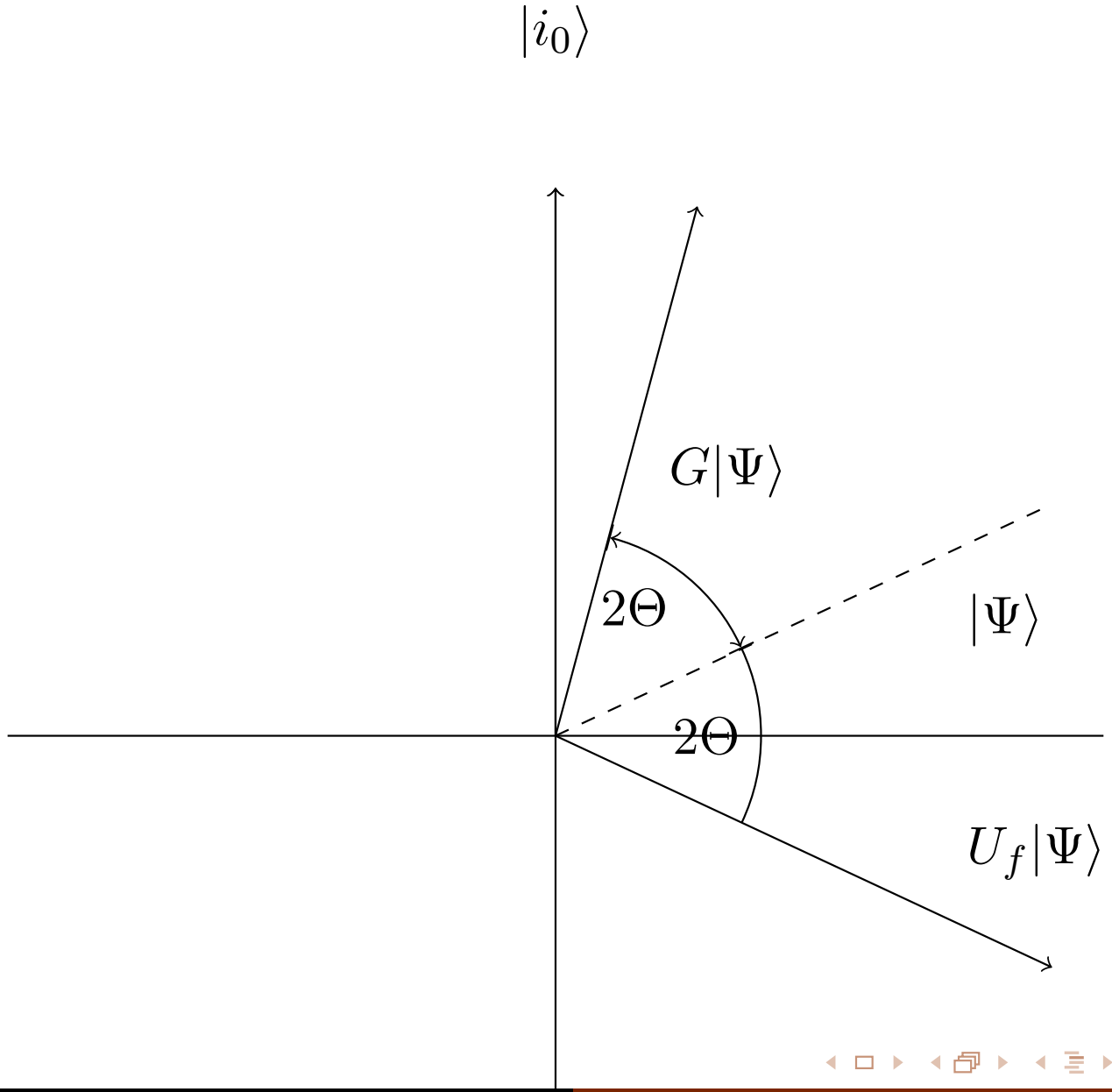
Grover operator

$$D = \begin{bmatrix} \frac{2}{N} - 1 & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} - 1 & \cdots & \frac{2}{N} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} - 1 \end{bmatrix} \tag{2}$$

Rotation des Vektors in Richtung Lösungsvektor

Definition

Bei dieser Betrachtungsweise sieht man sich an, wie der Vektor des Gesamtsystem unter Anwendung des Grover Operators in Richtung Lösungsvektor $|i_0\rangle$ rotiert. Als Basisvektoren werden bei dieser Darstellung der Lösungsvektor $|i_0\rangle$ und $|\Psi\rangle$.


$|i_0\rangle$
$G|\Psi\rangle$
2Θ
$|\Psi\rangle$
2Θ
$U_f|\Psi\rangle$

Auswirkungen der einzelnen Operatoren

- $\cos 2\Theta = \langle \Psi | \Psi_o \rangle = 1 - \frac{1}{2^{n-1}}$
- $\cos 2\Theta' = \langle \Psi | \Psi_G \rangle = 1 - \frac{1}{2^{n-1}}$

Es ist zu sehen, dass $2\Theta' = 2\Theta$. Daher rotiert der Vektor $\rangle|\Psi\rangle$ um 4Θ im Uhrzeigersinn in Richtung $|i_0\rangle$.

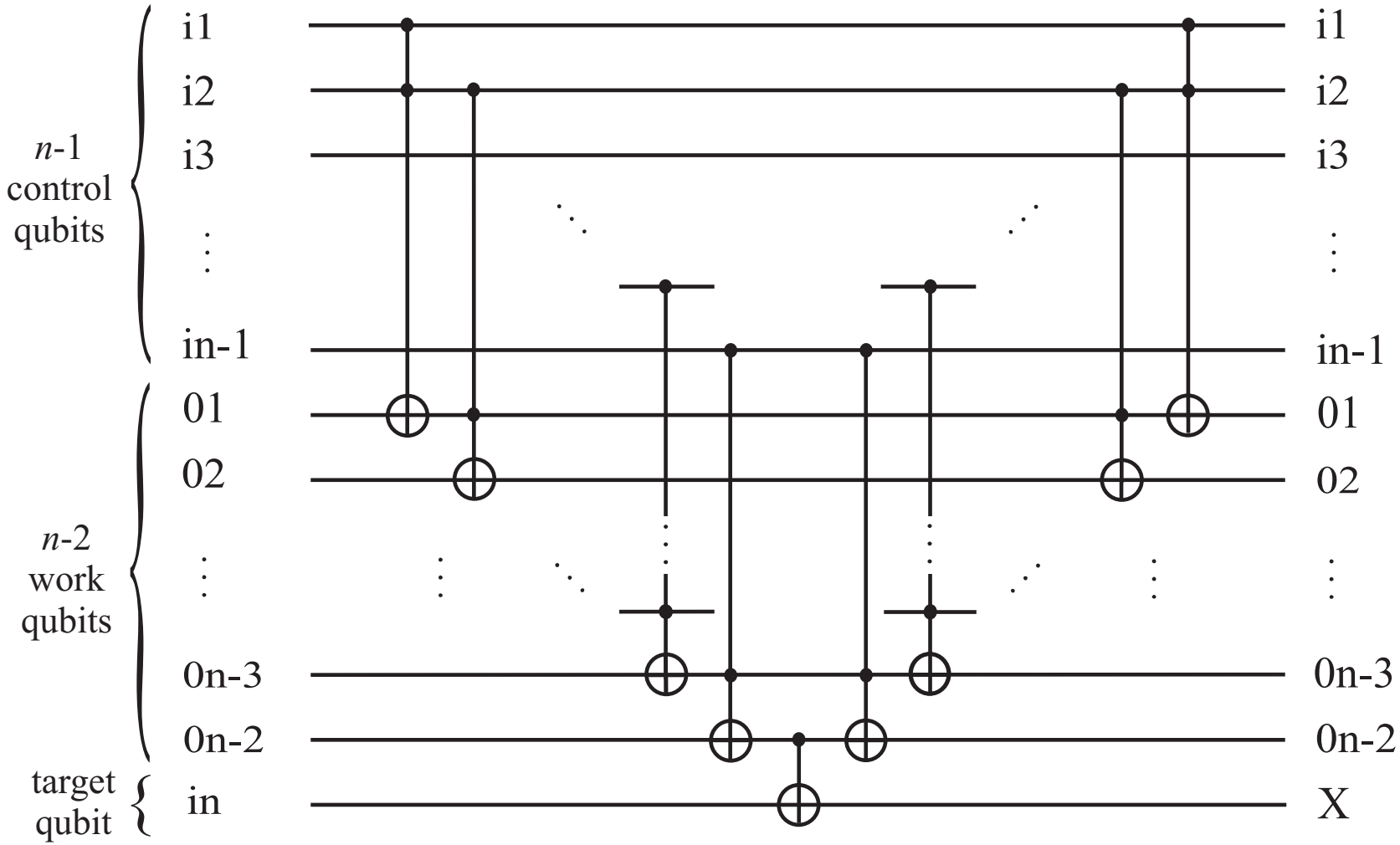
Anzahl an Iterationen

Die Anzahl an Grover Iterationen damit das gesuchte Element mit maximaler Wahrscheinlichkeit zurückgegeben wird ist

Ideale Anzahl an Iterationen

$$k = \frac{\pi}{4}\sqrt{N} \tag{3}$$

Verallgemeinertes Toffoli Gate



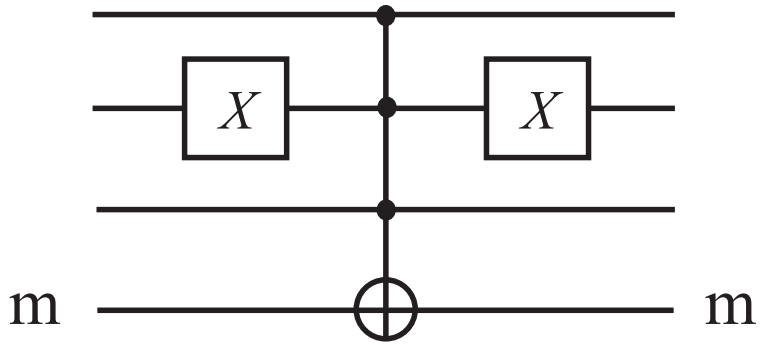


Abbildung: Decomposition of $I - 2\left|101\right\rangle\left\langle 101\right|$, which simulates U_f that searches number 5.

Grover Operator

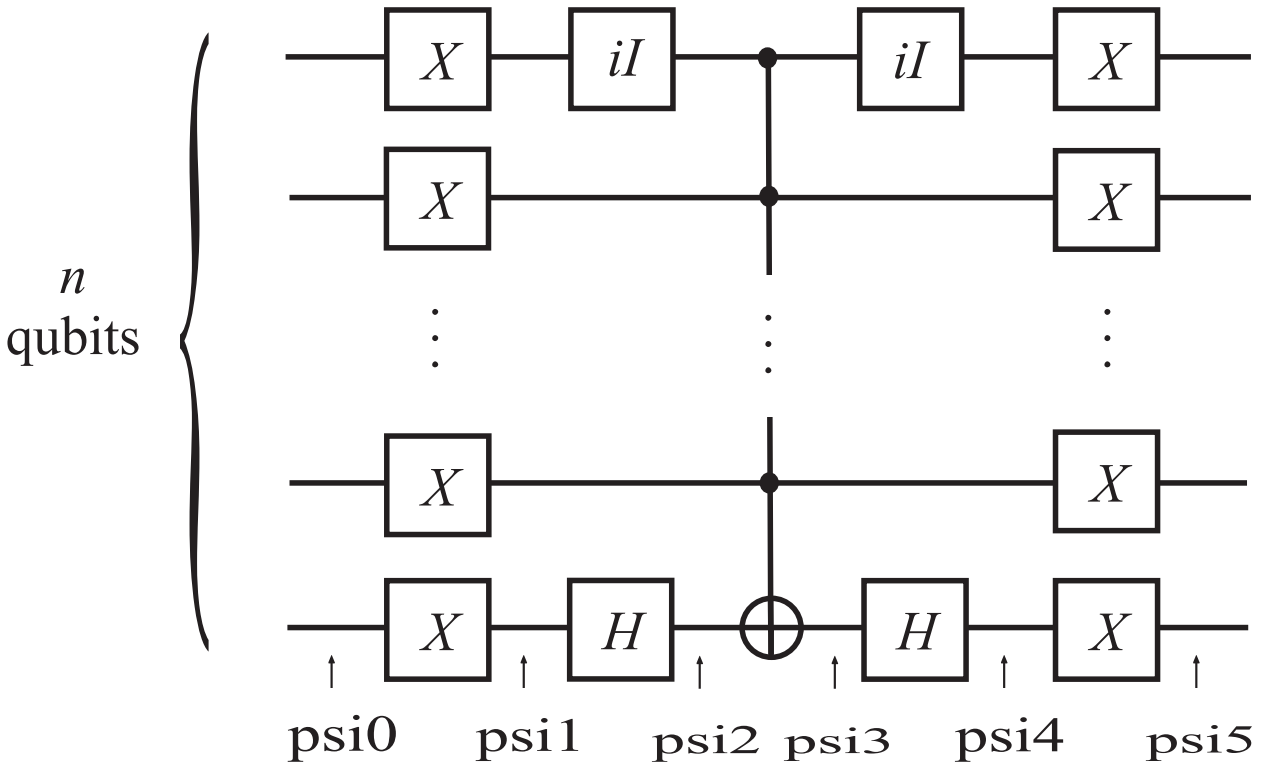


Abbildung: Circuit for $2\left|0\right\rangle\left\langle 0\right| - I$. Note the presence of the imaginary unit, which does not affect the real character of the operator.

Grover Algorithmus in Quantengattern

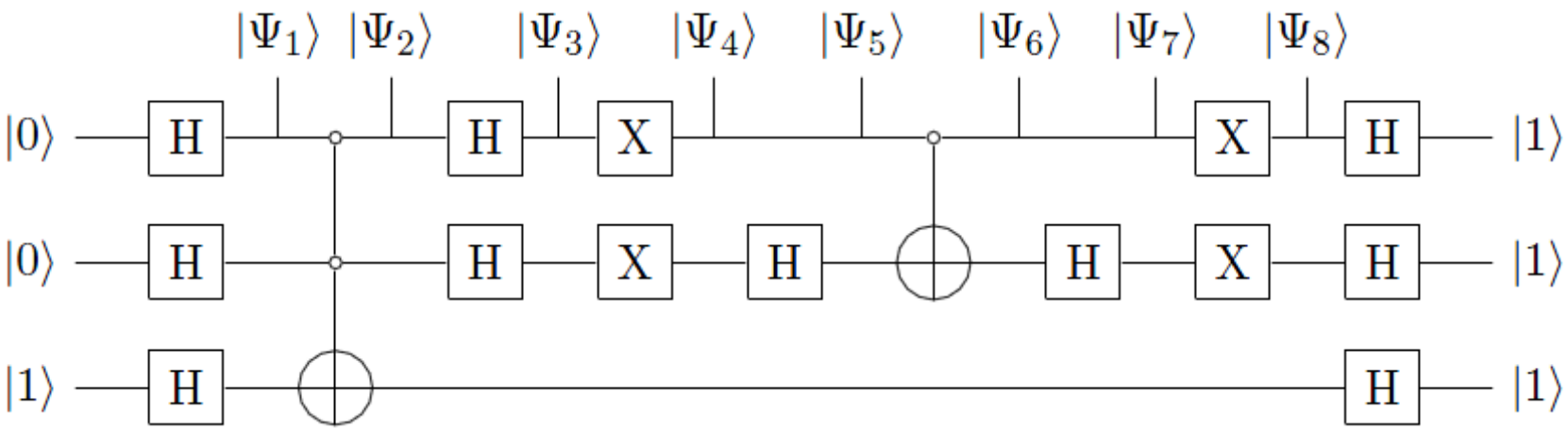


Abbildung: Searching state $|11\rangle$ using quantum gates

Ausgangssituation

- System besteht aus 2 Qubits
- Gesucht ist das Element $|11\rangle$
- Das Datenregister: $|\Psi\rangle = |00\rangle$
- Das Hilfsregister: $|1\rangle$
- Für Lösung wird nur eine Iteration benötigt
- Nach einer Iteration erhält man das gesuchte Element zu 100%

$|\Psi_1\rangle$

$$|\Psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

Das erste Register befindet sich nun in einer Superposition

$|\Psi_2\rangle$

$$
\begin{aligned}
|\Psi_2\rangle &= \frac{1}{2}[(|00\rangle + |01\rangle + |10\rangle)(|0\rangle - |1\rangle) + |11\rangle \\
&\quad (|1\rangle - |0\rangle)] \\
&= \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle - |11\rangle\right)
\end{aligned}
$$

Nach Anwenden des Orakels ist der entsprechende Zustand mit negativer Amplitude versehen worden.

$|\Psi_3\rangle$

$$
\begin{aligned}
|\Psi_3\rangle &= \frac{1}{4}[(|0\rangle + |1\rangle)(|0\rangle + |1\rangle) + (|0\rangle + |1\rangle)(|0\rangle - |1\rangle) \\
&\quad + (|0\rangle - |1\rangle)(|0\rangle + |1\rangle) + (|0\rangle - |1\rangle)(|0\rangle - |1\rangle)] \\
&= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)
\end{aligned}
$$

Nun sind 2 Hadamard-Gatter auf die ersten zwei Qubits anzuwenden.

$|\Psi_4\rangle$

$$|\Psi_4\rangle = \frac{1}{2}\left(|11\rangle + |10\rangle + |01\rangle - |00\rangle\right)$$

Da nach dem Zustand $|11\rangle$ gesucht wird müssen NOT-Gatter auf beide Qubits angewendet werden

$|\Psi_5\rangle$

$$
\begin{aligned}
|\Psi_5\rangle &= \frac{1}{2\sqrt{2}}[|1\rangle(|0\rangle - |1\rangle) + |1\rangle(|0\rangle + |1\rangle) \\
&\quad + |0\rangle(|0\rangle - |1\rangle) - |0\rangle(|0\rangle - |1\rangle)] \\
&= \frac{1}{\sqrt{2}}\left(|10\rangle - |01\rangle\right)
\end{aligned}
$$

In diesem Schritt wurde ein Hadamard-Gatter auf das zweite Qubit angewendet

$|\Psi_6\rangle$

$$|\Psi_6\rangle = \frac{1}{\sqrt{2}} \left(|11\rangle - |01\rangle \right)$$

Hier wurde das Controlled-NOT Gatter angewendet.

$|\Psi_7\rangle$

$$|\Psi_7\rangle = \frac{1}{2}[|1\rangle(|0\rangle - |1\rangle) - |0\rangle(|0\rangle - |1\rangle)]$$
$$= \frac{1}{2}(|10\rangle - |11\rangle - |00\rangle + |01\rangle)$$

Wieder das Hadamard-Gatter auf zweites Qubit

$|\Psi_8\rangle$

$$|\Psi_8\rangle = \frac{1}{2}(|01\rangle - |00\rangle - |11\rangle + |10\rangle)$$

NOT-Gatter auf die zwei Qubits im Datenregister angewendet

$|\Psi_9\rangle$

$$
\begin{aligned}
|\Psi_9\rangle = \frac{1}{4}[&(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) - (|0\rangle + |1\rangle)(|0\rangle + |1\rangle) \\
&- (|0\rangle - |1\rangle)(|0\rangle - |1\rangle) + (|0\rangle - |1\rangle)(|0\rangle + |1\rangle)] \\
= \frac{1}{4}&(4|11\rangle) = |11\rangle
\end{aligned}
$$

Auf alle Qubits wurden Hadamard-Gatter angewendet

Das Ergebnis

wie erwartet wurde der Zustand bereits nach einer Iteration mit einer Wahrscheinlichkeit von 100% gefunden.

Danke für Ihre Aufmerksamkeit

Danke für Ihre Aufmerksamkeit